NEW YORK STATE CYBERSECURITY STRATEGY

AUGUST 2023

Governor Kathy Hochul

Foreword by Governor Kathy Hochul

As Governor of New York State, I am proud to present our first-ever cybersecurity strategy. Cybersecurity and resilience are not just technical issues; they are essential to public safety and economic security.

This strategy unifies New York State's cybersecurity services, functions, and operations to better protect our critical infrastructure, personal information, and digital assets from malicious actors. It also provides a framework for aligning the actions and resources of both public and private New York stakeholders so that we can collectively work toward a shared vision for protecting New York. Key among those stakeholders are county and local governments, which are often the primary interface between New York's residents and many government services.

New York State's Chief Cyber Officer will oversee the implementation of this strategy. I created the position of Chief Cyber Officer in 2022 to centralize the State's management of cybersecurity and resilience activities. Successful implementation will require continued teamwork and coordination across State agencies and between Federal, state, tribal, and local governments, as well as the private sector.

Our cybersecurity strategy represents a significant step toward better protecting New Yorkers from digital threats. By taking a unified approach to cybersecurity and resilience throughout New York State, we can defend against threats and respond more quickly to potential attacks. I want to thank everyone who was consulted and made contributions to this strategy. I look forward to working together to implement it and create a safer, more secure New York.

Governor Kathy Hochul

Introduction

The safe and secure functioning of our economy, critical infrastructure, and government services depends on our ability to protect digital infrastructure and sensitive information. However, as global cyberattacks increase in both frequency and sophistication, fueled in part by the professionalization of the global cybercrime industry, we must raise the bar for what is necessary to successfully defend systems and networks.

The New York Cybersecurity Strategy sets forth an approach to cybersecurity and resilience based on the principles of unification, resilience, and preparedness. By bringing together the capabilities, resources, and insights of disparate stakeholders into a unified statewide approach, New York is better able to reduce the ability of malicious cyber actors to hold New York residents, businesses, and infrastructure at risk.

This strategy outlines Governor Hochul's plan for ensuring that New Yorkers continue to reap the benefits of the digital age while remaining protected from digital threats.

This strategy is organized into the following sections:

1. A Convergence of Cyber Threats
2. New York's Approach: Unification, Resilience, and Preparedness
3. Critical Stakeholders
4. Strategic Pillars: Operate, Collaborate, Regulate, Communicate, and Grow

A Convergence of Cyber Threats

New Yorkers face a wide array of malicious cyber activities, including exposure to ransomware and extortion attacks, state-sponsored and industrial espionage, intellectual property theft, and denial of service attacks. These attacks range from nuisances that temporarily slow websites to the disruption of vital services like healthcare.

Cyber threats are marked by a convergence of criminal and nation-state actors. Nation-states increasingly rely on cyber criminals to execute state actions. Those criminals, in turn, continue to perpetrate crimes, aided by additional resources and technical capabilities. This blending of criminal and nation-state malicious activity has increased the magnitude and complexity of cyber threats.

Cyber Criminals

The Federal Bureau of Investigation estimated that more than 25,000 New Yorkers were the victims of cybercrimes totaling $777 million in losses in 2022, making New York third in the nation in total victim losses by state.[1] In recent years, the technical sophistication and organizational maturity of cyber criminals has increased as cyber criminals have become better resourced and organized.

This maturity is most evident in the continued evolution of ransomware attacks. Ransomware attacks occur when a criminal encrypts a victim's files, systems, or networks and threatens to keep them locked until the victim pays a ransom. Cyber criminals have evolved from executing attacks as individuals to selling specialized expertise and capabilities to other criminals, allowing well-organized criminal organizations to buy scalable ransomware services in the same way legitimate businesses purchase information technology services. Today, ransomware attacks increasingly consist of double extortions where criminals seek payment both for the decryption of locked data and for refraining from posting sensitive or embarrassing stolen data.

Nation-State Actors

Nation-state actors—foreign intelligence and military services as well as nation-state-affiliated criminals—also threaten New York. Nation-state attackers may seek to conduct espionage, steal sensitive intellectual property, or disrupt critical infrastructure in a time of crisis or to inflict economic and societal damage on the United States. The U.S. has determined that both China and Russia pose significant cyber threats to the United States, stating in 2023 that China "almost certainly would consider undertaking aggressive cyber operations…that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."[2]

1. Federal Bureau of Investigation, Internet Crime Report 2022, March 2022.
2. Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, February 6, 2023.

Russia demonstrated its ability to compromise critical infrastructure in February 2022 when it conducted a series of disruptive cyberattacks against government systems and networks in advance of its invasion of Ukraine. Russia also temporarily degraded a privately owned satellite communications system used for Ukrainian military and government communications. Since then, Russian government-backed attackers have continued to target Ukrainian military and civilian infrastructure with destructive malware, some of which has extended to other countries allied with the U.S. The U.S. Intelligence Community has determined that Russia is "focused on improving its ability to target critical infrastructure…in the United States, as well as in allied and partner countries." [3]

3. Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, February 6, 2023.

New York's Approach: Unification, Resilience, and Preparedness

This strategy seeks to ensure all New Yorkers are better protected from digital threats by making New York more:

- ***Unified,*** *by working to increase access to cybersecurity information, tools, and services so that the State's most sophisticated defenses are available to its least-resourced entities.*
- ***Resilient,*** *by moving to expand the scope of cybersecurity regulations, requirements, and recommendations so that New York's critical infrastructure is better protected.*
- ***Prepared,*** *by providing advice and guidance to ensure New Yorkers are empowered to take charge of their own cybersecurity.*

These measures will help to level the cybersecurity playing field and ensure New York's defense is greater than the sum of its parts.

This strategy also acknowledges that cybersecurity and resilience are collective public, private, and individual responsibilities. Breaches that span thousands of devices and multiple networks often come down to a single opened email or file. Every New Yorker has a role to play in cybersecurity, from an employee at a State agency to a resident seeking to access government services via the Internet.

Critical Stakeholders

New York State has a complex ecosystem of public, private, and non-profit organizations that each play a significant role in cybersecurity awareness, preparedness, response, and mitigation. This strategy depends on the actions of each stakeholder and their contribution to New York's defense and resilience.

Principal cybersecurity stakeholders include:

- **New York State Chief Cyber Officer:** The Chief Cyber Officer reports to the Director of State Operations and Infrastructure and is the principal advisor to the Governor for reducing cyber risk, managing significant cyber incidents, and increasing cybersecurity and resilience in New York State.
- **New York State Division of Homeland Security and Emergency Services (DHSES):** DHSES provides leadership, coordination, and support to prevent, protect against, prepare for, respond to, recover from, and mitigate disasters and other emergencies. DHSES is responsible for working with Federal, state, local, and private entities to protect the State's critical infrastructure from cyber threats and vulnerabilities and to coordinate and facilitate information sharing and intelligence amongst these entities to assist in the early detection of, and response to, natural and man-made disasters.
- **New York State Office of Information Technology Services (ITS):** ITS operates State networks on behalf of many executive agencies. The ITS Chief Information Security Officer (CISO) provides cybersecurity support and assistance to agencies, conducts around-the-clock cybersecurity monitoring

and operations, manages an incident response team, and promulgates policies, standards, and programs relating to cybersecurity and resilience

- **New York State Police (NYSP):** NYSP operates the New York State Intelligence Center (NYSIC), a multi-agency, all-crimes fusion center that identifies, prevents, and protects New York against threats. The NYSIC Cyber Analysis Unit (CAU), provides cyber threat intelligence, outreach, analysis, and support. NYSP also operates the Computer Crime Unit (CCU), which provides outreach and education to community groups, training to law enforcement agencies, and administers the Internet Crimes Against Children Task Force (ICAC), which identifies, investigates, and prosecutes individuals who use the internet and technology to exploit children.
- **New York State Division of Military and Naval Affairs (DMNA):** DMNA is the State's executive agency responsible for managing New York's Military Forces, including its Cyber Protection Team (CPT). The CPT is jointly staffed and managed by the New York and New Jersey National Guard in support of State and Federal missions. DMNA also provides full-time State Active Duty Service Members to augment and coordinate training, security assessments, and incident responses for government agencies and critical infrastructure.
- **New York State regulatory agencies:** Regulatory agencies are responsible for ensuring critical infrastructure owners and operators meet minimum statewide requirements for safety, security, and resilience.
- **County and local governments:** County and local governments are responsible for the cybersecurity and resilience of their own information technology environments. They partner with the State, industry, non-profits, and other local governments to share threat information and best practices. They can expect the State to collaborate with them to disrupt malicious cyber actors, provide grant funding to modernize their information technology environments, and, when requested or directed, provide cyber support.
- **Critical infrastructure owners and operators:** Critical infrastructure operators manage their own systems and networks and are responsible for their own cybersecurity and resilience. They can expect the State to collaborate with them to disrupt malicious cyber actors, regulate them to ensure the security of critical services New Yorkers rely on, and, when requested or directed, provide cyber support.
- **Public schools, colleges, and universities:** New York's interconnected system of educational services range from K-12 to colleges and universities. They are presided over by the Board of Regents, comprised of members elected by the State Legislature. Schools and educational institutions can expect the State to provide advice and guidance about cybersecurity and resilience best practices and, when requested or directed, provide cyber support.
- **New York businesses:** Businesses in New York manage their own systems and networks and are responsible for their own cybersecurity and resilience. They can expect the State to share information with them to disrupt malicious cyber actors, regulate them to ensure the privacy of New Yorkers, and provide advice and guidance about cybersecurity and resilience best practices.
- **New York residents and visitors:** New Yorkers, and visitors to New York, own and operate their own devices and are responsible for their own cybersecurity and resilience. They can expect the State to provide them with advice and guidance about how to reduce the risk from malicious cyber actors and how to react in the event public services are severely disrupted.

The State also maintains a close partnership with neighboring states and the Federal Government for cyber threat information sharing, incident response coordination, and combined planning.

Strategic Pillars: Operate, Collaborate, Regulate, Communicate, and Grow

This strategy is composed of five mutually reinforcing strategic pillars.

The pillars are:

1. ***Operate*** State Government networks securely and resiliently.
2. ***Collaborate*** with key stakeholders.
3. ***Regulate*** critical industries.
4. ***Communicate*** cybersecurity advice and guidance.
5. ***Grow*** New York's cybersecurity workforce and economy.

Pillar 1: Operate State Government Networks Securely and Resiliently

New York State Government systems and networks must be secure and resilient while delivering services and functioning efficiently. The State is continuously working to consolidate and update its information technology infrastructure, operations, and policies. The State will continue these efforts with a renewed focus on updating and expanding its defensive capabilities, modernizing the State's network architecture in accordance with zero trust best practices, and preparing to address the threats to encryption posed by quantum computing.

Enhance the New York Security Operations Center

The New York Security Operations Center (NY SOC) is a state-of-the-art hub for collecting data from State agencies and other participating partners, operating statewide security monitoring tools and investigating suspicious activity.

In recent years, the State has made substantial investments in NY SOC capability and capacity to allow the NY SOC to update its technical cybersecurity tools, hire more technical specialists, and improve facilities. Going forward, the State will focus on exercising and operating the NY SOC, investing in new cybersecurity tools as necessary, further integrating the NY SOC into the overall State incident response process, and enhancing and adding NY SOC facilities. Adding more sites will not only ensure continuity of operations in an emergency, but will also allow the State to expand its potential talent pool.

Assess and Track Risk at State Agencies

The State evaluates cybersecurity risk across its systems and networks using a variety of tools and processes. The State will enhance these existing assessment efforts to evaluate and mitigate risk to State agencies and to offer risk assessment tools to non-executive entities. This process will allow the State to appropriately prioritize new investments in capabilities, operations, or other components of agency cybersecurity programs.

Assessing cybersecurity risk at State agencies that control operational technology (OT) is of particular importance in ensuring the cybersecurity and resilience of critical infrastructure. OT systems manage and control physical processes, meaning that cyberattacks that impact OT functionality can have immediate and tangible physical impacts, including operational disruptions, equipment malfunctions, and even physical damage. The State will continue to assess cybersecurity risks at agencies that operate OT to prioritize areas for future investment.

Modernize State Networks According to Zero Trust Principles

The State is continuously updating its networks and systems to improve resilience, reliability, and security based on the principles of zero trust. The foundational tenet of the zero trust approach is that no user, system, network, or service operating outside or within the network is inherently trusted; anything attempting to establish access must be verified on a periodic or continuous basis to establish or maintain access to data, systems, networks, or services.

The State's implementation of zero trust builds upon its core competencies in endpoint security, identity management, and application and service delivery.

The State will continue to press forward with its modernization efforts, including by enhancing its existing capabilities in order to continuously manage assets and enhance network segmentation.

A major focus for future zero trust implementation will be updating legacy software, hardware, and operational paradigms with new systems that offer better performance and security. When it is appropriate to do so, the State will accelerate efforts to replace legacy systems throughout its digital footprint.

Issue Updated Cybersecurity Policies

The New York State Technology Law empowers ITS to establish policies, standards, programs, and services relating to the security of State government networks. All State agencies are required to adhere to these statewide technology policies and standards, and these documents are made publicly available as a resource for local governments and other entities to use as templates or references for their own information technology and cybersecurity and resilience programs.

ITS will continue to review and, where necessary, update its existing policies to ensure they keep pace with changes to the threat environment and the state-of-the-art for cybersecurity and resilience technologies.

Pillar 2: Collaborate with Key Stakeholders

The State will collaborate with key stakeholders, including city, county, tribal, and local governments, private sector partners, and non-profit organizations, to increase cybersecurity and resilience across New York.

Provide Cybersecurity Services to County and Local Governments

The resources and expertise required to defend against cyber criminals and nation-states have evolved along with the sophistication of attacks. These greater demands pose a particular challenge for local governments, which may be unable to obtain leading-edge cybersecurity products and hire dedicated cybersecurity personnel.

The State has taken steps to augment the cybersecurity of county and local governments in order to raise New York's overall cybersecurity posture. The DHSES Cyber Incident Response Team (CIRT) supports local governments, non-executive agencies, and public authorities by providing free cyber incident response and

proactive cybersecurity services, including cybersecurity risk assessments, phishing programs, tabletop exercises, and cyber capability workshops.

Last year, the State initiated a new program to provide shared cybersecurity tools and services to county and local governments. The Shared Services Program is designed to offer county and local governments with differing levels of technological maturity potential access to the same high-value tools.

The first service offered via the Shared Services Program is an endpoint detection and response (EDR) capability. EDR solutions detect suspicious behavior on devices (e.g., desktops, laptops, servers) connected to a network. Data from the EDR solution is automatically shared with the NY SOC, creating, for the first time, a way for the State to incorporate malicious cyber activity targeting county and local governments into its overall statewide threat picture.

Moving forward, the State will endeavor to expand the availability of the EDR service and continue to refine the Shared Services Program operating model. The State will also work to make additional cybersecurity tools available to county and local governments, as appropriate.

Build a Statewide Picture of Cyber Threats

The State builds its situational awareness of statewide cyber threat activity in three ways: by monitoring State systems and networks, by monitoring alerts from county and local government networks provided via the State's Shared Services Program, and by processing reports submitted from external entities to State agencies about malicious cyber incidents. The State uses this information to create a comprehensive statewide threat picture that benefits all New Yorkers through the generation of threat reports that are disseminated to stakeholders.

The Shared Services Program is a key contributor to the statewide threat picture. By voluntarily sharing their threat-related data, participating county and local governments afford the State the opportunity to identify and correlate malicious cyber activity across multiple independent information technology environments. This information also feeds threat reporting that is distributed to a wider audience.

The State disseminates actionable information derived from all its data sources via the NYSIC and the Joint Security Operations Center (JSOC).

The NYSIC is a multi-agency fusion center that leverages its investigative and analytic resources and subject matter expertise to disseminate finished cyber threat reporting statewide. The NYSIC was established to collect, analyze, and disseminate intelligence related to criminal and terrorist activities, including in cyberspace, and to enhance information sharing and collaboration among Federal, state, local, and tribal law enforcement agencies, as well as private sector partners.

The JSOC was formed in 2022 in partnership with the cities of Albany, Buffalo, New York City, Rochester, Syracuse, and Yonkers to facilitate the exchange of information and analytical collaboration among participants.

Going forward, the State will continue to refine the processes and procedures employed by the JSOC to share threat information, facilitate analytical exchanges, and enhance operational collaboration amongst its participants.

Conduct Outreach to Strategically Important Companies & Institutions

New York is home to many companies and research institutions working at the leading edge of strategically important industries, including semiconductor manufacturing, biotechnology, aerospace, and cybersecurity. These industries are priority targets for foreign intelligence services seeking to obtain products and technologies for strategic and commercial advantage, including via cyber espionage. Earlier this year, the U.S. Intelligence Community determined that "China will persist with efforts to acquire foreign science and technology information and expertise, making extensive use of…cyber theft to acquire and transfer technologies and technical knowledge." [4]

The State will continue to work with partners in the Federal Government to raise awareness about the risk of cyber espionage, intellectual property theft, and threats to companies and institutions in New York. In addition to educating companies about how to identify and mitigate cyber and counterintelligence risks, the State will continue its outreach to businesses to facilitate the rapid reporting of any suspicious activity.

Provide and Administer Grants

The State provides grants to county and local government entities for information technology modernization and cybersecurity purposes, including via the DHSES Homeland Security Preparedness Programs and NYS Department of State's Local Government Efficiency (LGE) grant program.

The State also leverages Federal grant funding to enhance cybersecurity statewide. In 2021, the U.S. Congress passed the Infrastructure Investment and Jobs Act (IIJA), which included a provision establishing the State and Local Cybersecurity Grant Program (SLCGP) to help state, local, and territorial governments address cybersecurity risks and threats to their information systems. The State will continue to leverage this and other related Federal grants in order to assist local government entities in managing and reducing cyber risk.

Pillar 3: Regulate Critical Industries

New Yorkers need to know that the critical infrastructure they rely on is secure from disruption by cyberattack. Regulations ensure that infrastructure owners and operators are meeting, or exceeding, the minimum level of security necessary to protect the vital services they deliver. The process of developing regulations and policies that may affect the security of critical infrastructure will continue to be informed by existing Federal cybersecurity frameworks, as applicable.

Financial Sector

In 2017, the New York State Department of Financial Services (DFS) became the first banking or insurance regulator in the nation to establish a cybersecurity division to protect consumers and industries from cyber threats. DFS also created first-in-the-nation requirements for DFS-regulated banks, insurance companies, virtual currency companies, and other financial services institutions. The State will continue to build on the success of these cybersecurity regulations through amendments to ensure they keep pace with new threats and technologies, as applicable.

Energy Sector

In 2022, the Governor signed legislation creating strongest-in-the-nation cybersecurity protections for New York's energy grid by requiring electric distribution utilities to prepare for cyberattacks in their annual emergency response plans by providing the New York Public Service Commission (PSC) with enhanced

4. Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, February 6, 2023.

auditing powers. The State will partner with electric distribution utilities and the U.S. Department of Energy (DOE) on the implementation of this new law.

Pillar 4: Communicate Cybersecurity Aduice and Guidance

Many New Yorkers may not be aware of the cyber threats they are vulnerable to, the actions they could take to secure their systems and their information, or what to do if they are a victim of a cybercrime. The State provides information to New York residents and businesses to empower New Yorkers to take charge of their own cybersecurity and to respond appropriately in a crisis.

Issue Cyber Hygiene Guidance

Low-sophistication attacks can often be prevented by taking simple actions, such as regularly updating software and operating systems to patch known vulnerabilities, using strong passwords and multi-factor authentication, and avoiding clicking on unexpected or suspicious links. To help ensure New Yorkers receive actionable guidance about how to protect themselves online, the State will continue to regularly issue basic cyber hygiene guidance including via social media.

In addition, the State publishes advice and guidance tailored to focused audiences, such as local governments and financial institutions. This guidance provides the target audience with an authoritative source for specific cybersecurity information.

Foster Communities of Practice

Engagement with local governments is critical to advancing statewide cybersecurity. A statewide, unified approach relies on trusted relationships among State and local leaders. Working across organizational boundaries towards a single vision means fostering both formal and informal intergovernmental communities for sharing cybersecurity practices and insights.

The State will continue its efforts to facilitate cyber awareness and preparedness information sharing and engagements with a range of key stakeholder groups, including local government associations representing information technology leaders. These engagements serve to facilitate coordination, collaboration, and the development of statewide cyber skills and capabilities.

Pillar 5: Grow New York's Cybersecurity Workforce and Economy

The State is working to increase New York's cybersecurity talent pool both to make New York a preferred hiring destination for companies and institutions and to ensure that State agencies and other governments throughout New York can hire and retain the cybersecurity personnel they need.

Expand the Talent Pool for Public and Private Employers

A highly skilled cybersecurity workforce is key to continuing to grow the technology industry in New York, one of the Governor's primary economic goals, as well as ensuring that New York businesses and governments can hire the people they need to secure themselves from cyber threats.

The State is continuing to invest in the State University of New York (SUNY) to ensure that New York is a center for cybersecurity talent and a draw for businesses and public institutions alike. The State is making significant investments in expanding several SUNY institutions into hubs for high-technology research and centers for Federal research funding, including by building lab facilities and deepening partnerships with relevant private sector partners.

In addition, the State is providing extra resources to school districts, boards of cooperative educational services (BOCES), and community colleges to develop strategic plans that better align high school and college academic offerings with the workforce requirements of New York employers, including technology and cybersecurity firms.

At the high school level, the State is expanding programs, such as the New York State Pathways in Technology Program, that create opportunities for high school students to gain valuable expertise in high-skill jobs, including technology. The State is partnering with educational organizations to create cybersecurity curriculum materials for use at K-12 and higher education institutions.

Minimize Barriers for Hiring and Retaining State Talent

The Governor's budget for FY2024 includes landmark funding for New York's civil service system that will make it easier to hire, and retain, skilled technical talent. These changes include a continuous recruitment initiative to allow agencies to accept applications continuously for a variety of titles, add to the pool of qualified candidates at more regular intervals, and offer recruitment exams on an ongoing basis via a hybrid of online testing and in-person assessments.

The State will continue to leverage fellowship programs, including the Empire State Fellows Program and the Excelsior Service Fellowship Program, to place recent graduates and experienced professionals in technology-focused positions. These programs provide an additional pipeline for candidates from backgrounds that are historically underrepresented in the technology industry.

The State is also working to increase its talent pool by offering greater geographic flexibility to its employees by opening new office locations for information technology workers. These additional locations will provide these personnel with the flexibility to live and work throughout New York.

Finally, the State is committed to balancing the business needs of agencies with the flexibility needed by employees by permitting telecommuting where possible. As part of this effort to add workplace flexibility, the State is modernizing State office spaces and adopting new technology that accommodates the needs of telecommuters while improving agency operations.

Conclusion

New York's first ever statewide cybersecurity strategy provides a framework for unifying the cybersecurity and resilience activities of stakeholders as part of a cohesive approach to driving down cyber risk across the State.

This strategy provides a framework to unify the State's capabilities, resources, and policies to ensure that New York is better protected from the increasingly sophisticated and impactful cyberattacks that threaten our economic security and public safety.

This strategy also prioritizes cybersecurity education and workforce development to ensure that New Yorkers of all backgrounds can contribute to the critical mission of cyber defense. Building an equitable talent pipeline to both the public and private sectors is a requirement for successfully defending New York's digital terrain.


NEW
YORK
STATE